REMARKS

Claims 1-4 remain in the Application.

The Office Action rejected Claims 1-4 as being anticipated under 35 U.S.C. §102 by *Tsunoo et al.* (European Patent App. No. 0932272 A2, hereinafter "*Tsunoo*").

The present invention seeks to provide an estimate as to the strength of a cipher and also to reduce the amount calculations necessary to find session keys for plural rounds of ciphers such as DES or MISTY. It accomplishes this by a calculating session key prospect for a given round and then using the calculated session key prospect for a given round to calculate session key prospects for other rounds. This reduces the number of calculations necessary because there is a greater likelihood of success when the session key prospects for rounds are found using other session key prospects for other rounds rather than finding all of the session key prospects individually. (Spec. Pages 4 – 5). The amount of calculation and the number of pairs of plaintext and ciphertext which are required to find the session key are displayed as indicators for estimating the strength of a cipher. (Spec. Page. 18).

Tsunoo aims to provide an encryption strength evaluation support apparatus that is capable of evaluating encryption strength independent of any specific decoding method and finely analyzing the behavior of encryption conversion. It takes the individual bits of the input and output data of an encryption device and performs statistical analysis on the correlation between the individual bits. (¶¶ 0017-18). This can include bit balance, output bit correlation, input bit-output bit correlation, and avalanche. (¶ 0026). It then edits the data and outputs it in the form of a table or a 2-D or 3-D graph. (¶¶ 0018-19). As seen in Figure 17A, the higher the value of [count of inversion – count of non-inversion], the higher the "mountains" and the lower the value of [count of inversion – count of non-inversion], the lower the "valleys." The higher

mountains means that the corresponding an input and output have a high correlation, and a deep valley means that the correlation is extremely low, both of which are non-desirable properties. On the other hand, a field indicates that to probability of an output bit being inverted when an output bit is inverted is close to 0.5, which is a good property. This allows an operator to quickly and intuitively analyze the behavioral details of the encryption algorithm. (¶ 0112; Fig. 17A).

With respect to Claims 1-3, *Tsunoo* does not teach or suggest the feature of "an untransformed text calculating unit and a control unit, the untransformed text calculating unit comprising a session key prospect calculating section and an untransformed text calculating unit body." *Tsunoo* does not disclose calculating a session key prospect or a putative untransformed text. *Tsunoo* is only interested in performing a statistical analysis between the individual bits of the input and output data rather than figuring out the session key. (¶¶ 0017-18; 26).

In contrast, the present invention has a putative untransformed text calculating unit 2 which receives a putative transformed text and outputs a putative untransformed text for a given round for a cipher such as MISTY while calculating a session key prospect in-between. As can be seen in Figure 1 of the present invention, in the process of calculating the putative untransformed text, the session key prospect calculating section 2B receives a plaintext and putative transformed text to calculate a session key prospect which it sends to the putative untransformed text calculating unit body 2A. The putative untransformed calculating unit body 2A receives a putative transformed text and uses the session key prospect from the session key prospect calculating section 2B to calculate the putative untransformed text for a given round.

Thus the present invention can not only estimate the strength of a cipher, but it can also calculate session key prospects, and reduce the number of calculations necessary to find the session key for a cipher.

Furthermore, for Claim 4, *Tsunoo* also fails to disclose "the cipher strength estimating device comprising a first untransformed text calculating unit, a second untransformed text calculating unit, and a control unit, the first untransformed text calculating unit comprising an untransformed text calculating unit body and a first session key prospect calculating section, the second untransformed text calculating unit comprising a second session key prospect calculating section." *Tsunoo* does not disclose calculating a first session key prospect, a second session key prospect, or a putative untransformed text. *Tsunoo* is only interested in performing a statistical analysis between the individual bits of the input and output data rather than figuring out the session key. (¶¶ 0017-18; 26).

In contrast, in the present invention, the plaintext and ciphertext calculating unit 3 chooses a pair of plaintext and ciphertext which is suitable for applying higher order differential cryptanalysis to the modified MISTY that is to be evaluated. The control unit 1 then inputs the plaintext and ciphertext from the plaintext and ciphertext calculating unit 3 to the first untransformed text calculating unit 21. The first session key prospect calculating 21K receives the ciphertext and plaintext and calculates a 6^{th} round session key prospect utilizing the brute-force search method. (Spec. pg. 17; Fig. 4).

The untransformed text calculating unit body 20A included in the first untransformed text calculating unit 21 receives the ciphertext and the 6^{th} round session key prospect and calculates a putative untransformed text which is presumed to be equivalent to a 6^{th} round output. (Spec. pg. 17; Fig. 4).

The control unit 1 receives the 6^{th} round putative untransformed text and inputs the putative untransformed text as a 5^{th} round putative transformed text to the second untransformed text calculating unit 22 along with the plaintext. (Spec. Page 18; Fig. 4). The second

untransformed text calculating unit 22 receives the plaintext and the 5th round putative transformed text and creates conditions for calculation of a 5th round session key prospect dynamically. (Spec. Pages 13-14; Fig. 4). It accomplishes this by creating plural Boolean polynomials for dynamically calculating a session key prospect based on the 5th round putative transformed text and creating plural conditions. If the plural conditions for calculating a session key prospect include conditions that are inconsistent with each other, the second session key prospect calculating section 22k outputs uncalculability identifier data indicative of an inability to calculate the session key prospect. (Spec. Page 14-16; Fig.4).

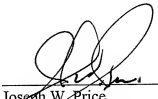
If there is a recalculation request based on receipt of uncalculability identified data, the control unit 1 outputs the recalculation request data to the first session key prospect calculating section 21K. The first session key prospect calculating section 21K then calculates another 6th round session key prospect and outputs a 6th round putative untransformed text based on the newly calculated 6th round session key prospect. (Spec. Page 18; Fig. 4). The calculation of the 6th round session key prospect is repeated until the session key prospect for the 5th round is obtained. Since the 5th round session key prospect finally obtained can be considered equivalent to the session key in terms of probability, the amount of calculation and the number of pairs of plaintext and ciphertext, which have been required to find the session key, are displayed in the display as indicators for estimating the strength of the cipher.

Thus the present invention can not only estimate the strength of a cipher, but it can also reduce the number of calculations necessary to find the session key for a cipher. (Spec. pg. 18)

If the Examiner believes that a telephone interview will help further the prosecution of this case, the Examiner is respectfully requested to contact the undersigned attorney at the listed telephone number.

Very truly yours,

SNELL & WILMER L.L.P.



Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626
Phone: (714) 427-7420
Fax: (714) 427-7799